Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
XM WWW.XM.COM USAIN BOLT OFFICIAL SPONSOR

SECURITY

Cryptocurrency like bitcoin is easy money for criminals

Bitcoin and its brethren have earned a reputation for fast returns on investment, but they're vehicles for exploitation too.

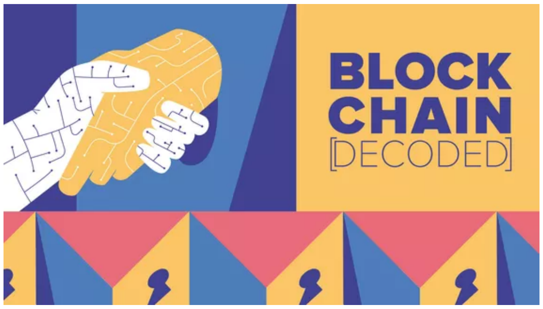
BY **ALFRED NG** / FEBRUARY 14, 2018 5:00 AM PST

SAVE 44% ON YOUR SUBSCRIPTION
LEARN MORE
NIKKEI ASIAN REVIEW

Aaron Robinson/CNET

This is part of "Blockchain Decoded," a series looking at the impact of blockchain, bitcoin and cryptocurrency on our lives.

The Winklevoss twins aren't the only ones getting rich off cryptocurrency. Criminals are raking it in too.



See more from Blockchain Decoded.

Thanks to the meteoric rise of bitcoin over the past year, you've probably heard of cryptocurrency, or digital money that uses blockchain encryption technology for transaction security. By mid-December, the value of one bitcoin reached more than $19,000. It's since fallen below $7,000, though it's recovered some ground over the past week.

Get your
$30
Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
XM WWW.XM.COM | USAIN BOLT OFFICIAL SPONSOR

Bitcoin is the best-known cryptocurrency on the market. However, there are more than 1,500 cryptocurrencies out there, some with goofy names like Dogecoin, PinkDog and Californium.

Before you get too excited about using or trading this new form of money, be aware that cryptocurrencies are rife with criminal activity. Cryptocurrency, for instance, is the preferred form of payment when hackers lock up your computer for ransom, such as in last year's widespread WannaCry attack. Likewise, there are viruses that turn computers into slave machines mining for cryptocurrency. Hackers have also created malware disguised as cryptocurrency apps, tricking folks who think they're cashing in on the trend.

"It's usually being used for something illegal," said Steve McGregory, the application and threat intelligence director at security firm Ixia. He estimates that 99 percent of illegal activities online use cryptocurrency.

BLOCKCHAIN DECODED

Blockchain ensures that your online baby food order is legit

What is bitcoin? Here's everything you need to know

Blockchain explained: It builds trust when you need it most

Buying and selling bitcoin, explained

This is cryptocurrency's dark side, which sometimes gets lost in the hype over the rocketing value of bitcoin and its brethren. But just as digital currency has turned into a hot new investment vehicle, it's given hackers and cybercriminals new opportunities for exploitation.

Even old-school cons have taken a new blockchain twist, with consumers excitedly buying new forms of cryptocurrency only to find they're little more than hot air and false promises.

"With cryptocurrency, it's like choose-your-own adventure," said Rick Holland, a cybercrime researcher at security company Digital Shadows. "People can pick so many routes to target victims now."

Hide the money

The reasons that cryptocurrency has become a trusted, valued form of money are the same reasons it has become an invaluable asset for cybercriminals, who want to get paid for their efforts.

All cryptocurrency transactions use a mix of public and private keys to keep payments secure and, in some scenarios, completely secret. You can see where the money goes and which wallets its headed to. But if you can't link the wallet to a person, the identity remains secret.

Watch this: Cryptojacking: The hot new hacker trick for easy money 1:43

That anonymity allows cybercriminals to sell information from massive breaches, such as the 145.5 million Social Security numbers stolen from Equifax or data from 3 billion hacked Yahoo accounts, without worrying about law enforcement tracking who's buying or selling it. Likewise, the WannaCry hackers demanded victims each pay $300 worth of bitcoin to get their devices back to normal last year. Criminals even use cryptocurrency to pay for online classes that teach ways to use stolen credit card numbers.

"The cryptocurrency world allowed bad guys to start collecting in ways that made them less vulnerable to being identified or caught," said Michael Kaiser, the former executive director of the National Cyber Security Alliance.

That cover has helped boost the ranks of cybercriminals, despite the nascent efforts of governments to crack down. For example, the European Union and the UK are working to crack down on the anonymous nature of cryptocurrency, out of concern that it helps terrorist groups and their money-laundering efforts.

"We should be looking at these very seriously precisely because of the way they can be used, particularly by criminals," British Prime Minister Theresa May told Bloomberg last month.

Get your
$30
Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
XM WWW.XM.COM | USAIN BOLT OFFICIAL SPONSOR

Dorado
30% BONUS
CLOCK IS TICKING...
Buy tokens
get 30% bonus

The EU plans to require platforms where bitcoins are traded to report suspicious sales and to monitor users, while the UK wants officials to oversee online transactions. In November, Stephen Barclay, then-economics secretary to the UK treasury, said the government expects these changes to take effect this year.

Get your
$30
Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
XM
WWW.XM.COM
USAIN BOLT
OFFICIAL SPONSOR

Banking on botnets

Botnets, a mass of hijacked computers under the control of a hacker, were once primarily used to fire off spam emails or initiate distributed denial-of-service attacks, which essentially block a website by overwhelming it with traffic.

But with cryptocurrency, hackers found another purpose for botnets: making money.

Cryptocurrency is bought and sold, but it must also be mined, or verified, with immense computing power. Given the processing chops needed to mine cryptocurrency, the cost of the electricity to run the machines can be higher than the mining revenue. But if you're not using your own computer, there's little expense eating into your profits. When the Mirai botnet hit in 2016, hackers took control of thousands of connected devices around the world.

"We were expecting DDoS attacks, but then we started seeing loads of people dropping bitcoin-mining payloads on the routers and cameras," McGregory said. "If you get thousands of these, you can make money off of someone else's machine and it's easy pickings."

McGregory spotted malware designed to stay hidden on hacked machines and mine for cryptocurrency in the background. If you owned one of these computers, the effect would be a dramatic slowdown in performance. And that wasn't even a sophisticated attack.

Mining malware is sold online for as cheap as $35, according to security researchers from Recorded Future.

McGregory said mining apps in the Google Play Store have been downloaded more than 10 million times. He's found them in fake puzzle games, crosswords and tic-tac-toe apps. He's also spotted one called Reward Digger, in which the player earns virtual coins but in actuality is helping hackers mine bitcoin.

Mugging malware

If you can't mine cryptocurrency or get a botnet to do it for you, there's always the old-fashioned way: stealing it.

Some malware searches for cryptocurrency wallets and empties them via virtual burglary. In October, antivirus company Kaspersky Lab researchers discovered CryptoShuffler, a trojan that lets hackers change the wallet address from a victim's computer to their own, essentially diverting the funds away from the intended person.

Get your
$30
Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
XM WWW.XM.COM
USAIN BOLT OFFICIAL SPONSOR

Because of the anonymity of transactions, a victim doesn't know what happened until it's too late. Since Kaspersky discovered it, the trojan has stolen 23 bitcoins, now worth around $210,000.

"Lately, we've observed an increase in malware attacks targeted at different types of cryptocurrencies, and we expect this trend to continue," Sergey Yunakovsky, malware analyst at Kaspersky Lab, said in a statement.

In December, NiceHash, another cryptocurrency mining marketplace, said it had been hacked to the tune of $62 million. And unlike money stolen from a bank, police can't find it and victims won't ever get it back.

Old crimes, new tech

The connection between cryptocurrency and crime is only going to get worse as investments continue to boom.

The US Securities and Exchange Commission last year cracked down on a cryptocurrency scheme that it said raised more than $15 million before it was busted. The alleged scammers promised wild returns on the launch of a new digital currency, but the SEC said that investments went toward their personal expenses instead.

Holland predicts that it'll be five to 10 years before governments can get a handle on digital currency crimes, and even then it may not be possible. That's because the schemes will just evolve.

"It's a new twist on an old game," Holland said. "But now the scale at which you can do this is high and the likelihood of you being busted is low."

The Smartest Stuff: Innovators are thinking up new ways to make you, and the things around you, smarter.

Virtual reality 101: CNET tells you everything you need to know about VR.

YOU MAY ALSO LIKE Sponsored Links by Taboola

How To Start Online Business In Philippines & See Results In 2017

Sponsored by Project Ignited

What Reese Lansangan Does with That "Rush from Being in an Unfamiliar Place"

Sponsored by Cosmo for Ford

The Ultimate Cheap Flights Finder is Here!

Sponsored by Save70.com

New Site Finds the Cheapest Flights in Seconds!

Sponsored by FlightFinder

Get your
$30
Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
XM WWW.XM.COM | USAIN BOLT OFFICIAL SPONSOR

SHARE YOUR VOICE

24 comments

TAGS

Blockchain Decoded

Security

Bitcoin

Hacking

Next Article: Your quote tweets make bad tweets worse. Do this instead

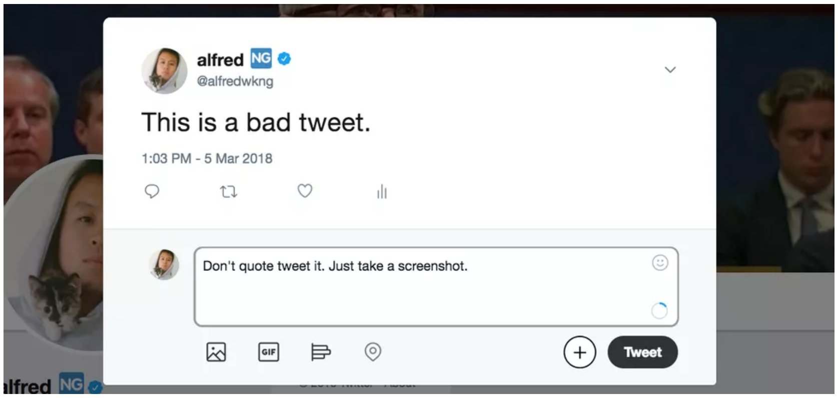
AdChoices
manawa Get a FREE IT Assessment

CULTURE

Your quote tweets make bad tweets worse. Do this instead

Critics denouncing Parkland shooting conspiracy theories ended up fanning the flames on social media. Here’s how you can criticize without amplifying.

BY **ALFRED NG** / MARCH 6, 2018 5:00 AM PST


alfred NG
@alfredwkng

This is a bad tweet.

1:03 PM - 5 Mar 2018

Don't quote tweet it. Just take a screenshot.

Taking a screenshot is better than quote-tweeting a post you're speaking out against.

Alfred Ng/CNET

Algorithms on social media don't care if you share something because you're for it or against it.

And if you're against it, your post could backfire.

A share is a share, and it only serves to draw more attention to the post you're arguing against, despite your best intentions, social media experts say. That's why when four prominent accounts on Twitter, including former first daughter Chelsea Clinton, last month shared a conspiracy theory post tied to the Parkland, Florida, high school shooting in order to denounce it, they ended up fueling the fire instead of putting it out.

> **Chelsea Clinton**
> @ChelseaClinton
>
> Jim - could you please return to attacking me (or really any grownup) instead of the courageous #Parkland students? Thank you. twitter.com/gatewaypundit/…
>
> 8:33 AM - Feb 20, 2018
>
> 133K 26.8K people are talking about this

The four tweets ended up accounting for more than 60 percent of the total mentions on the original story, according to Wired, bringing attention to what is essentially a fake news take on the shooting. But experts say there are better ways to criticize something on Twitter. Stop engaging, whether it's through a quote-tweet or a share. Just take a screenshot.

"If you have a very large following, quote-tweeting it is spreading it and problematic," said Jennifer Grygiel, a social media professor at Syracuse University. "You should try to reference it without perpetuating it."

When about a quarter of American adults get their news from social media, quote-tweets and retweets can end up influencing news feeds for millions of people.

Outrage machine

Creating outrage has become a common plan of attack for trolls on social media: Any attention is good, and controversy courts reactions.

It's the same playbook Russian trolls from the Internet Research Agency used when they set out to disrupt the US presidential election in 2016. The trolls masked themselves as activists speaking on behalf of Black Lives Matter and gun rights groups and posted the most divisive content they could. The angry responses pretty much guaranteed that their posts and tweets would pop up on news feeds. Twitter said 1.4 million people were exposed to Russia propaganda on its platform. Facebook said the disinformation reached 126 million people.

Facebook and Twitter didn't respond to requests for comment.

> “
> If you have a large audience, with that comes responsibility.
>
> Jennifer Grygiel, professor, Syracuse University

On Feb. 16, US Special Counsel Robert Mueller filed an indictment against the IRA for its trolling efforts tied to the 2016 election. He charged 13 Russians involved with using Facebook and Twitter for "information warfare."

Two weeks later, Twitter CEO Jack Dorsey acknowledged his site's problems with trolls and online harassment, writing that the company "didn't fully predict or understand the real-world negative consequences." He also acknowledged that people have been taking advantage of Twitter's algorithms and is asking the public to submit proposals on how his company can improve.

"Bad actors know that if they say something that incites others, it'll drive up their post," said Cliff Lampe, a social media professor at University of Michigan's School of Information. "It creates an incentive for them to say something offensive."

Bearing witness

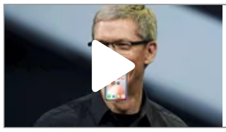
So how does this all work in a world where it's also important to be able to criticize content on social media, especially since silence can be misinterpreted as acceptance? Calling out bad takes is an integral part of holding voices online accountable.

"We're all bearing witness to these tragedies, and just remaining silent doesn't help pushing forward social change. It doesn't help advocate for social justice issues," Grygiel said.

Taking a screenshot of the tweet you're criticizing may be a more effective way to reference it without giving the post a social boost -- you're cutting off engagement to the original source.

Turns out screenshots are also a pretty effective archiving tool for social media.

For a while on Twitter, people who misspoke were leaving their inaccurate tweets alone, arguing that this was a way to "preserve the record" even as they also posted a correction. Taylor Lorenz of the Daily Beast suggested instead taking a screenshot of your incorrect tweet, deleting the original and posting the screenshot with your correction.



Watch this: How to spot fake news 3:21

The problem with that approach is that trolls can exploit it to make matters worse, not better. After the mass shooting at the Florida high school, trolls Photoshopped a tweet by a Miami Herald reporter to make it appear she'd asked for videos of "dead bodies." She did not.

People are also quick to trust screenshots, even if it's ridiculous stuff.

When the Twitter joke account Pixelated Boat tweeted a doctored excerpt from Michael Wolff's book "Fire and Fury," claiming President Trump watched the "Gorilla Channel" 24 hours a day, it quickly trended on Twitter and even fooled several analysts.

So you need to make sure screenshots aren't fake, which adds extra work to finding the truth. But taking that extra step is worth it if you want to avoid inadvertently helping to popularize a message you're actually criticizing.

"If you have a large audience, with that comes responsibility," Grygiel said. "If it takes you a couple more seconds to do it in a way that will not perpetuate harm, then you need to do that."

iHate: CNET looks at how intolerance is taking over the internet.

Security: Stay up-to-date on the latest in breaches, hacks, fixes and all those cybersecurity issues that keep you up at night.

SHARE YOUR VOICE

7 comments

TAGS

Culture Twitter

Next Article: Uber trucks in Arizona? Yeah, and they're self-driving, too

CNET Magazine

Check out the Spring 2018 issue of CNET Magazine, where you'll learn how our digital gadgets could testify against us in court, discover how to take great vacation photos with your phone, and spend time with Jesse Tyler Ferguson of "Modern Family," who says he's just trying to get a handle on the fast-changing digital world we live in.

Read Now!

Download the CNET app / About CNET / Privacy Policy / Ad Choice / Terms of Use / Mobile User Agreement / Help Center

© CBS INTERACTIVE INC.
All Rights Reserved.

AFFILIATE DISCLOSURE
CNET earns commissions from retail offers.

TOP BRANDS